Air Defense Artillery

USAADASCH Quarterly OPSEC Newsletter

Volume 1, Issue 1
July 1, 2005

America's role as the dominant political, economic, and military force in the world makes it the Number 1 target for foreign espionage. As FBI Director Louis Freeh has reported to Congress, foreign intelligence activities against the United States have grown in diversity and complexity since the end of the Cold War. In addition to the intelligence services of friendly as well as unfriendly countries, sources of the threat to classified and other protected information include:

- Foreign or multinational corporations.
- Foreign government-sponsored educational and scientific institutions.
- Free-lance agents (some of whom are unemployed former intelligence officers).
- Computer hackers.
- Terrorist organizations.
- Revolutionary groups.
- Extremist ethnic or religious organizations.
- Drug syndicates.
- Organized crime.

The intelligence services of friendly and allied countries are now more active in intelligence operations against the United States than during the Cold War. Espionage by friends in addition to adversaries has long been more widespread than generally realized.

OPSEC focuses on identifying and protecting information that might provided a competitor or adversary with clues to our plans or capabilities, and thereby enable the competitor or adversary to thwart a planned operation or activity.

Please email comments to the address below, we'd love to here from you.

opsec2 @bliss.army.mil

Operations Security (OPSEC)

Volume 1, Issue 1
July 1, 2005

OPSEC is the shorthand term for operations security. OPSEC is not a specific category of information. Rather, it is a process for identifying, controlling, and protecting generally unclassified information which, if it becomes known to a competitor or adversary, could be used to our disadvantage.

The OPSEC process is applied to a wide variety of situations in a competitive or adversary environment. If you have ever given a surprise party or attempted to make your house look lived in while you were away, by arranging for someone to pick up your newspapers or installing a light timer, you have practiced OPSEC. The following are just a few examples of things that, under certain circumstances, might provide clues that tip off a competitor or adversary to your plans or capabilities: supply and equipment orders, transportation plans, mission-specific training, changes in communication patterns, leaders' travel, inspection results.

OPSEC is used by government agencies and contractors in the development and acquisition of new equipment, in intelligence collection, by war fighters at all levels, by crime fighters in many roles, as well as by private enterprise -- all to supplement traditional security measures for protecting potentially exploitable information.

Have you seen me ?

Here's an Eye-Popper *& it's not from Popeye's*

During the past 20 years, Americans have been arrested and convicted of spying for South Korea, Taiwan, Philippines, Israel, Greece, Saudi Arabia, Iraq, Jordan, Ghana, Liberia, South Africa, El Salvador and Ecuador -- in addition to Russia, the former Soviet Union, China, and the various formerly communist countries.

In many cases, foreign targets in this country have not changed. "There is still a deadly serious interest in 'traditional' intelligence activities such as penetrating the U.S. intelligence community, collecting classified information on U.S. military defense systems, and purloining the latest advances in our country's science and technology sector."

Source

Defense Security Service

It's no use saying, "We are doing our best." You have got to succeed in doing what is necessary.

Winston Churchill

How Do I Know When I'm Being Targeted and Assessed?

The likelihood of you being targeted for initial assessment usually depends upon circumstances over which you have little or no control. Circumstances that increase the chances include the following.

- *Your access to information, people, or places of active intelligence interest.*
- *Travel abroad where foreign intelligence operatives can gain access to you on their home turf.*
- *Work in a position or geographic location in the U.S. where it is easy for foreign nationals to gain access to you or your family.*
- *Ethnic, racial, or religious background that may attract the attention of a foreign intelligence operative.*

Hum, what do these Americans have for us today

Air Defense Artillery

USAADASCH

Fort Bliss
Texas 79916

Phone: 915-568-4675

SBU what is it and how do we protect it?

The term Sensitive But Unclassified information as used here is an informal designation applicable to all those types and forms of information that, by regulation, require some form of protection but are outside the formal system for classifying national security information. As a general rule, all such information may be exempt from release to the public under the FOIA. This section will review the most common types of sensitive unclassified information.
Department of Army also uses the term Controlled Unclassified Information (CUI) to refer to certain types of sensitive information within the Army that require controls and protective measures. CUI includes FOUO and information with comparable designations that is received from other agencies.
Generally speaking, the law provides protection for established categories of protected information only when the owners of the information have taken reasonable or required steps to protect it. These steps are sometimes stated in the regulation; however, they are often left up to the information owner to develop internally.

Key elements to a successful information protection program:

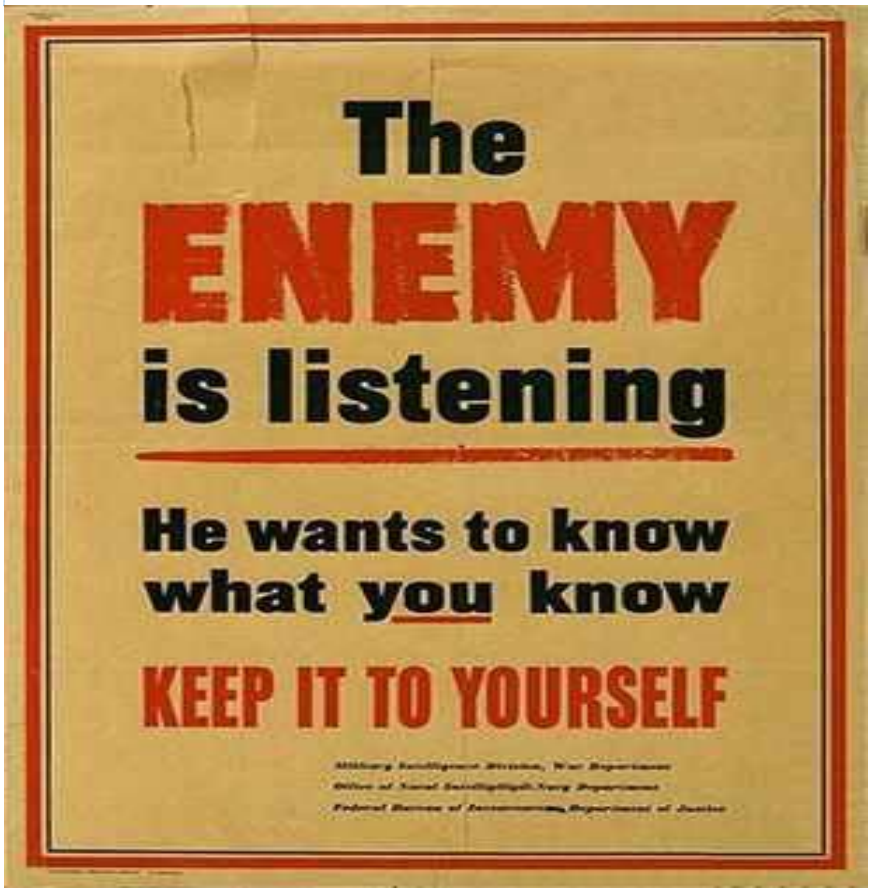
- An established information SOP.
- A system to identify the specific information to be protected. What are your EEFI's.
- Procedures for safeguarding and controlling the protected information so that it is exposed only to those who have a need to know the information and a duty to protect it. The duty to protect may be imposed by regulation (for some categories) or established by a confidentiality in others.

- Proper marking and classification of documents.

Factors affecting the implementation are the degree of sensitivity of the information, nature of the threat to the information, vulnerability of the information, options that are available for protecting the information, and organizational capabilities for secure handling, storage and transmission.

Please email comments to the address below, we'd love to hear from you.

opsec2@bliss.army.mil



Volume 1, Issue 1
July 1, 2005